IoT: Issues and Security challenges

Antar Saha*
Department of Computer Science and Engineering
Brainware University
antar.saha@yahoo.com

Sahabul Alam
Department of Computer Science and Engineering
Brainware University
sahabul2009@gmail.com

Abstract

Internet of Things (IoT) is being used in almost every segment of modern technology. For that reason many new ways are also discovered to make the IoT easier to connect and get benefitted from it. But as the usage is increasing, the security vulnerabilities are also increasing. One of the major problems of IoT technology is security. ***.*** *In this article, some common security issues and challenges involving IoT technology are highlighted.*

Keywords: IoT, security, Challenges

Introduction

Internet of Things technology connects to the Internet to all the smart devices such as sensor, smart devices. These devices are operated by the user's control. Internet to all devices, including resource limited sensors, as well as smart devices. In today's world, we are all connected with one another using our personal devices like smart phones, tablets, laptops and many other micro devices. All of them are working with the evolution of IOT (Internet of things). Basically IOT is being changed, more specifically developed day by day, and so that the experience of the end user is accelerating also. Now-a-days IoT is being used in almost every consumable device, from small smart phones/smart watches to large household accessories like washing machine, TV, AC etc. But as the technology is being developed, several kinds of issues, several kinds of challenges arises when the task is to protect the communication between devices and servers as well as making the data sharing as efficient as possible so that the communication becomes seamless, hassle-free and secure. As well as the underlying system (both server and client) need to be protected from being wrongly exposed to the outside internet. The IoT depends on wireless networks and provides connectivity of the smart devices. At present, Wireless technologies play an important role due to their mobility requirements (Abouzakhar, N. S., Jones, A., & Angelopoulou, O.,2017) .

For IoT security, there are several security probability. It should be considered security risk environments like smart devices that can be scaled on household appliances, healthcare, cars, as well as heterogeneous networks (Yunjung Lee, Y. P.,2015). All are connected to the Internet as well as cloud services. With the advancement of technology, the chances of security vulnerabilities also increases if proper updated security standards are not being followed. The paper is organized as follows: Section 2 provides related works. Section 3 gives issues and security challenges. Finally, section 4 gives a conclusion.

Related works

IoT is an emerging technology now-a-days. As the demand of automation is increasing day by day, many countries are now investing greatly to enhance the network of IoT. It will empower almost every segment of our everyday life including private business, personal works, government sections as well as households. (Yadav, E. P., Mittal, E. A., & Yadav, H.,2018)

Handheld devices are the most widely used mediums of IoT. A modern smartphone uses multiple types of sensors. They include Gyroscope, Proximity sensor, GPS and so on. They are being used for various purposes. But from a business perspective, they are being used by manufacturers to improve the User Experience (UX) as much as possible. The data is collected mainly in Cloud low latency storage containers like Firebase Firestore. This type of database has to be robust and flexible to capture and store streaming data in real bulk amounts and real time. Google's firebase firestore provides such a type of service combining with built in security and privacy. Also there are some services called Function as a Service (Faas) like Cloud Functions by Google Cloud Function (GCP) or Lambda by Amazon web service (AWS) which executes corresponding codes to post process these data is almost infinite scale and negligible latency (Sarkar, S., Gayen, S., &Bilgaiyan, S.,2018)

As the demand increases, the security needs to be increased also. Penetration testing is one of the testing metrics to measure the capability and efficiency of the architecture. This kind of techniques have some advantages over manual testing, like easy to manage the testing process, easy to monitor the test results, has the ability to mock almost every corner case situations, repeated random testing to check system capability etc. (Johari, R., Kaur, I., Tripathi, R., & Gupta, K., 2020)

This paper explores different technologies of IoT which can be used to build various IoT based products. These products are mainly used in enterprises to increase the user value. The backbone of IoT is cloud computing. IoT devices mainly sense environmental data and those data are stored in some storage services. Relational databases or NoSQL databases are mainly used to store these streaming data sent from IoT devices. Later these data are post processed to extract necessary analytics information or patterns for future use. Here cloud computing technologies play a vital role to store and process those data, at a very large scale. And now -a-days the costing of cloud computing resources has become very feasible that one has to pay only for the computing power and resources used, just like on-demand services. (Lee, I., & Lee, K. 2015) (Biswas, A. R., & Giaffreda, R. 2014, March)

Issues and Security challenges

The number of IoT devices usage is increasing every day. As well as new ways of breaking the existing security walls are also discovered by attackers. The main security issues of IoT are device security, data security, communication security as well as privacy. As the communication of the channels need to be authenticated so that there may not happen any unauthorized access to the nodes, on the other hand it also should be private, so that any intruder might not steal any communication or stored data. Some of the current issues of IoT technologies are in Table1.

Issues	Causes
Incorrect access control	- Same default password - Weak password - Lack of privileges
Large attack surface	- Insecure open ports - Proper port protection

Outdated software	- Device firmware version - Software version - Operating system version
Encryption	- Proper encryption on storage and medium - Proper authentication - Proper authorization
Application bugs	- Known application bugs - Unit testing
Execution environment	- Code signing - Digital signature
Physical security	- Unique security for each device

Table 1: Current issues of IoT

Some security challenges are:

Old operating system:
Every device that needs internet access, must run over an operating system. Day by day every operating system strengthens its security to fight against known vulnerabilities. So new versions are also released with necessary updates. But IoT devices, once set up, are hardly being updated to new releases of operating systems. This opens up a space to attackers to make the system attack easily.

Lack of Integrated Security:
Though the devices run an operating system, the underlying hardware specification is not that great to run an antivirus application like any other desktop computers. This increases the chance of attack by malwares which attack systems and steal sensitive data.

Hard to Patch or Update:
Another problem of having low end specifications is application update. Application softwares are developed in latest high end systems, though they are used in various scales of devices. But as time goes on, the consumables become so outdated that maintaining updates of those used application softwares for those low end devices become very problematic, so the updates are not maintained. Although released, almost many cases, that IoT device does not support that latest release because of hardware incompatibility.

Insecure Passwords:
Generally passwords are used as initial restrictions of IoT devices. Manufacturers by default set a password to that device. But they do not satisfy the latest security standards because those passwords are set up for demonstration whereas users most of the time use that default password as a regular one. Thus this increases the probability of guessing the passwords by the attackers.

Untrusted Deployment Locations:
Most of the IoT devices are designed to be used in public places, like CCTV cameras. In those cases, the security needs to be well planned so that any attacker cannot bypass the existing security walls to gain access to that device.

Use of Insecure Protocols:

Internet protocols are implemented to gain a layer of security when communicating between nodes over the internet. There are many protocols designed, some of them are deprecated also, like Telnet, because of its lack of built in security. But devices are well known for using these protocols for simplicity.

Conclusion

In this paper, we tried to review some security issues of IoT devices. Since the IoT has been invented, its popularity is getting increased because this technology opens up many scope of business opportunities. It also makes human life easier by giving the control of their consumables remotely and mainly through automation. Its popularity will increase in the future also. So if its security standards are maintained also in an well-defined way and if those are being followed by the manufacturers also, then the usage of the IoT devices may spread into some sensitive sectors also like core Government sectors, banking sectors and many other fields.

References

[1] Abouzakhar, N. S., Jones, A., & Angelopoulou, O. (2017, June). Internet of things security: A review of risks and threats to healthcare sector. In *2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)* (pp. 373-378). IEEE.

[2] Biswas, A. R., & Giaffreda, R. (2014, March). IoT and cloud convergence: Opportunities and challenges. *2014 IEEE World Forum on Internet of Things (WF-IoT).*

[3] Dorobantu, O. G., &Halunga, S. (2020, November). Security threats in IoT. In *2020 International Symposium on Electronics and Telecommunications (ISETC)* (pp. 1-4). IEEE.

[4] Garg, H., & Dave, M. (2019, April). Securing iot devices and securely connecting the dots using rest api and middleware. In *2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU)* (pp. 1-6). IEEE.

[5] Johari, R., Kaur, I., Tripathi, R., & Gupta, K. (2020, October). Penetration Testing in IoT Network. In *2020 5th International Conference on Computing, Communication and Security (ICCCS)* (pp. 1-7). IEEE.

[6] Sarkar, S., Gayen, S., &Bilgaiyan, S. (2018, July). Android Based Home Security Systems Using Internet of Things (IoT) and Firebase. In *2018 International Conference on Inventive Research in Computing Applications (ICIRCA)* (pp. 102-105). IEEE.

[7] Yadav, E. P., Mittal, E. A., & Yadav, H. (2018, February). IoT: Challenges and issues in Indian perspective. In *2018 3rd International Conference On Internet of Things: Smart Innovation and Usages (IoT-SIU)* (pp. 1-5). IEEE.

[8] Yunjung Lee, Y. P. (2015). Security Threats Analysis and Considerations for Internet of Things. In *2015 8th International Conference on Security Technology (SecTech)*.

[9] Lee, I., & Lee, K. (2015). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Business Horizons, 58*(4), 431-440.